## REMARKS

This responds to the Office Action mailed on May 20, 2005, and the references cited therewith.

Claims 1-20 are pending in this application.

### *§102 Rejection of the Claims*

Claims 1-7 and 9-19 were rejected under 35 U.S.C. § 102(b) as being anticipation by Carter et al. (U.S. Publication No. 2003/0051026 and Carter hereinafter). Claim 10 appears to be allowable as indicated on the Office Action Summary, and since no art was cited directly against it. Applicant reserves the right to swear behind the reference at a future date. The rejection is respectfully traversed.

The Office Action refers to paragraphs [0179] – [0183] of Carter et al., as disclosing the elements of claims 1, 3, and 13. Applicant has reviewed the referenced language and respectfully disagrees. The referenced language describes the analysis of attacks on a network. "The Network Surveillance and Security System uses artificial intelligence to detect and analyze attacks on servers in the protected network." [0180]. It references using inference engines, genetic learning algorithms and neural networks to perform the analysis of the attacks.

Claims 1-3 of the present application are not directed to analysis of attacks, but provide elements that facilitate the configuration of multiple different security software programs on a computer network. The claimed elements providing the ability to configure security software include a database engine providing deduction, a network information database, and a security goal database that describes uses that installed hardware and software may support. Further claims reference configuring multiple different types of security software packages based on security goals. These elements are not described in Carter et al., as Carter et al. is directed to monitor and protect the security of computer networks, learning from security events. Abstract.

The cited language in Carter et al., does not describe several of the elements of claim 1. Claim 1 recites a repository for configuration of hardware and software installed on the network. Carter et al., describes surveying host portion connections, detecting and disconnecting unauthorized intrusions,..." [0179] This language does not describe configuration of hardware and software, but deals with connections to ports, to find unauthorized connections. Claim 1 also

refers to a security goal database describing uses that the hardware and software installed on the network may support. No similar teaching was found in the cited language of Carter et al. Since several elements of claim 1 are lacking in Carter et al., the rejection should be withdrawn

The elements of claim 1 facilitate configuration of security software packages based on security policies, as indicated in the Summary of the present application. Carter et al., actually refers to the ability to "install the Network Surveillance and Security System without alterations to existing software or configuration files." [0183]. This appears to teach away from the presently claimed invention.

Claims 4-7 and 9 contain elements similar to claim 1, and are believed to distinguish from Carter et al. for at least the same reasons as claim 1. Further, claim 4 expressly recites elements that deal with configuration of security software packages utilizing the elements that are similar to claim 1. As described above, the citations to Carter et al., do not refer to configuring security software packages, and in fact describe not altering existing software or configuration files. The Office Action refers to the components of the Network surveillance and Security System accomplishing a variety of functional benefits for monitoring and protecting the security of a protected constellation. However, there is no citation to Carter et al., provided for this, and the statement does not appear to refer to configuration of security software packages. Thus, claims 4-7 and 9 are believed allowable, and withdrawal of the rejection is respectfully requested.

Claims 11 – 14 refer to configuring a security software package using one or more security goals. It also refers to decomposing security policies for a class into one or more security goals for an individual network device. The Office Action cites paragraphs [0179] to [0183] of Carter et al., as describing decomposing security policies. Applicant has reviewed the referenced language and respectfully disagrees. The referenced language describes the analysis of attacks on a network. "The Network Surveillance and Security System uses artificial intelligence to detect and analyze attacks on servers in the protected network." [0180]. It references using inference engines, genetic learning algorithms and neural networks to perform the analysis of the attacks.

The Office Action cites paragraphs [0975] to [0985] of Carter et al., as describing configuring software packages using the security goals. Applicant has reviewed the referenced

language and respectfully disagrees. The referenced language describes the use of agents to monitor protected constellations. The agents communicate reports back to the system. The system then configures a log "to report changes in security status within the protected constellation." [0977]. This language does not describe configuring a software package using security goals. Since multiple elements of claims 11-14 are not taught or disclosed in Carter et al., the rejection should be withdrawn.

Claim 15-16 distinguish from Carter et al. for similar reasons.

Claim 17 also refers to configuring the security software package, and is believed to distinguish from Carter et al. for similar reasons.

Claims 18-19 also refer to configuring the security software package, and are believed to distinguish from Carter et al. for similar reasons.

*Allowable Subject Matter*

Claim 10 was indicated as being allowable. Claims 8 and 20 were objected to as being dependent upon a rejected base claim, but were indicated to be allowable if rewritten in independent form including all of the limitations of the base claim and any intervening claims. Applicant has not rewritten the claims because they depend from claims which are now believed allowable.

## CONCLUSION

Applicant respectfully submits that the claims are in condition for allowance, and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicant's attorney at (612) 373-6972 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

Respectfully submitted,

ROBERT P. GOLDMAN ET AL.

By their Representatives,

SCHWEGMAN, LUNDBERG, WOESSNER & KLUTH, P.A.
P.O. Box 2938
Minneapolis, MN 55402
(612) 373-6972

Date 8-18-2005

By _____
Bradley A. Forrest
Reg. No. 30,837

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being deposited with the United States Postal Service with sufficient postage as first class mail, in an envelope addressed to: Mail Stop Amendment, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450, on this 18 day of August, 2005.

CANDIS BUENDING
Name

_____
Signature